REMARKS

The Office Action dated October 11, 2007, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-20 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 1-20 are currently pending and under consideration.

Claims 1-4, 7-9, 10, and 15-20 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0120328 to Adrangi et al. (Adrangi) in view of U.S. Patent Application Publication No. 2004/0120295 to Liu et al. (Liu). The Office Action took the position that Adrangi teaches some aspects of claims 1-4, 7-9, 10, and 15-20. The Office Action then cited Liu to cure the deficiencies of Adrangi. This rejection is respectfully traversed.

Independent claim 1, upon which claims 2-14 are dependent, recites a system that includes a mobile node belonging to a home network located within a secure network, the mobile node having a network interface configured to communicate with other nodes, the mobile node having only one security association and only one mobility binding with a home agent so as to provide secure mobile connectivity that implements a mobile internet protocol home agent functionality. The system also includes a proxy home agent connected to the home network and located within the secure network, wherein the proxy home agent is configured to provide a proxying functionality, the home agent located outside of the secure network, wherein the home agent is configured to provide a signaling and tunneling functionality and to notify the proxy home agent of the mobile node. The system further includes a virtual private network gateway located outside the secure network and configured to work in conjunction with the home agent.

Claim 15, upon which claims 16-18 are dependent, recites a method that includes establishing a proxy home agent located within the secure network to monitor data directed to the mobile node so as to secure communication between a mobile node associated with a home network in a secure network and a correspondent node. The method also includes establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the proxy home agent of the mobile node. The method further includes collecting data directed to the mobile node. The method additionally includes packaging the collected data in a virtual private network secure tunnel to an internal address of the mobile node to create virtual protocol network packaged data. The method also includes tunneling the virtual protocol network packaged data to a current address of the mobile node.

Claim 19 recites a system that includes means for establishing a proxy home agent located within a secure network to monitor data directed to a mobile node so as to secure mobile connectivity that implements mobile internet protocol home agent functionality via distributed components. The system also includes means for establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the proxy home agent of the mobile node. The system further includes means for collecting data directed to the mobile node and means for packaging the collected data in a virtual private network secure tunnel to an internal address of the mobile node to create virtual private network packaged data. The system additionally includes means for tunneling the virtual private network packaged data to a current address of the mobile node. The system also includes means for the home agent to communicate to the proxy home agent that the mobile node has moved outside its home network. The system additionally includes means for the home agent to communicate to the proxy home agent that the mobile node has come back to its home network. The system also includes means for enabling the proxy home agent to create and remove a proxy address resolution protocol entry for a permanent address associated with the mobile node.

Claim 20 recites a computer program embodied on a computer readable medium, the computer program being configured to control a processor to perform establishing a proxy home agent located within a secure network to monitor data directed to a mobile node. The computer program is also configured to control a processor to perform establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the proxy home agent of the mobile node, and collecting data directed to the mobile node. The computer program is further configured to control a processor to perform packaging the collected data in a virtual private network secure tunnel to an internal address of the mobile node to create virtual private network packaged data, and tunneling the virtual private network packaged data to a current address of the mobile node.

As will be discussed below, Adrangi and Liu fail to disclose or suggest the elements of any of the presently pending claims.

Adrangi generally describes a seamless, secure roaming solution across enterprise firewalls. Specifically, a mobile node (MN) 140 may register with a home agent ("HA 130") when it exits its home subnet. During the registration process, the MN 140 informs HA 130 of MN 140's "care-of address" (hereafter "COA"), namely MN 140's address on its new subnet. See paragraphs [0012]-[0013]. HA 130 thereafter intercepts all IP packets addressed to MN 140 and reroutes the packets to MN 140's COA. As MN 140 moves from one subnet to another, MN 140 may obtain new COAs via Dynamic Host Configuration Protocol ("DHCP") or other similar protocols.

To ensure that HA 130 is able to properly route packets to MN 140, MN 140 must continuously update HA 130 with its new COA as it roams on Corporate Intranet 100. This configuration is commonly referred to as a "co-located" communications mode. Alternatively, Adrangi provides that when MN 140 leaves its home subnet, it may register with HA 130 via a foreign agent (" FA 135") on MN 140's new ("foreign") subnet. By registering with FA 135, MN 140 may use FA 135's IP address as its COA when registering with HA 130. In this scenario, HA 130 continues to intercept all packets addressed to MN 140, but these packets are now rerouted to FA 135, namely MN

140's COA as provided to HA 130. FA 135 examines all packets it receives, and sends the appropriate ones to MN 140 at its current location on the foreign subnet.

It is respectfully submitted that Adrangi fails to disclose or suggest, at least, "the mobile node having **only one** security association **and only one** mobility binding with a home agent for providing secure mobile connectivity that implements a mobile internet protocol home agent functionality," as recited in independent claim 1. (Emphasis added) Instead, Adrangi discloses multiple possible mobility bindings with the Home Agent for the Mobile IP home agent. The Office Action referred to paragraphs [0023] - [0028] of Adrangi as describing this feature of independent claim 1.

However, in the referenced paragraphs, Adrangi provides that MN 140 registers with HAi 300 via the IPSec tunnel in 403, and provides HAi 300 with its care-of address (COAi, namely VPN Gateway 225's private address). MN 140 may then securely transmit IPSec-protected IP packets to nodes such as CN 310 on Corporate Intranet 100. Once MN 140 is registered with HAx and HAi, and IPSec Tunnel 315 has been established, MN 140 may send and receive IPSec-protected IP packets to and from CN 310. See paragraphs [0023] - [0028]. Contrary to the contentions made in the Office Action, paragraphs [0023] - [0028] do not teach or suggest that the MN 140 has "**only one** security association **and only one** mobility binding with the home agent for providing secure mobile connectivity that implements a mobile internet protocol home agent functionality." (Emphasis added)

The Office Action took the position that, on page 16, "while it is true that the "care-of" address (COA) of a mobile node [of Adrangi] may change during roaming, there is only one COA used for a mobile node at one time. Therefore, the current COA of a mobile node is the one and only one mobility binding used with a home agent of the mobile node at any given time." However, Adrangi clearly indicates that as the MN 140 moves from one subnet to another, MN 140 **may obtain new COA** via Dynamic Host Configuration Protocol ("DHCP") or other similar protocols. (Emphasis added) To ensure that HA 130 is able to properly route packets to MN 140, MN 140 of Adrangi **must continuously update HA 130 with its new <u>COAs</u> as it roams on Corporate Intranet 100**. (Emphasis added).

Furthermore, in view of the description provided in Adrangi that the MN 140 may obtain new "care-of" addresses and may continuously update with new "care-of" addresses. It is respectfully submitted that a person of ordinary skill in the art would not reasonably conclude that Adrangi describes "the mobile node having only one security association and only one mobility binding with a home agent (HA) for the mobile IP home agent functionality," as recited in independent claim 1. Also, Adrangi does not teach or suggest that the MN 140 uses only one security association as recited in independent claim 1.

In the response to arguments section, on page 16, the Office Action took the position that Adrangi teaches "the mobile node having only one security association and only one mobility binding with a home agent for the mobile IP functionality." The Office relies on the portion of the present application on page 10, lines 20-21 to support the rejection of claim 1. However, the Office Action's position is clearly erroneous because the Office Action merely relied on the description in the present application to reject independent claim 1, and the Office Action did not provide any specific support that Adrangi discloses or suggests that the mobile node includes **only one** security association and **only one** mobility binding with a home agent, as recited in independent claim 1.

It is respectfully submitted that Adrangi simply fails to teach or suggest, "the mobile node having **only one** security association and **only one** mobility binding with a home agent for the mobile IP functionality," as recited in independent claim 1. (Emphasis Added). Thus, it is respectfully requested the rejection of the independent claim 1 be withdrawn.

On page 4, the Office Action acknowledged that Adrangi does not teach or suggest, "wherein the home agent is configured to provide a signaling and tunneling functionality and to notify the proxy home agent of the mobile node," as recited in independent claim 1. Accordingly, the Office Action relied on Liu to resolve the deficiencies of Adrangi. Liu generally describes a method to provide a secure network path through an inner and outer firewall pair between a mobile node on a foreign network and a corresponding node on a home network. The Office Action refers to the description associated with FIG. 1A and paragraphs [0034] and [0035] of Liu as describing the signaling and tunneling functionality and notification recited in independent claim 1. However, the referred portion of Liu, and other portions of this reference, simply provides a filter rule constructor (FRC) 110 receiving an Access Control Listing (ACL) table 104 and a SITP mapping table 106 and generating a graph of filter chains 114. The control element downloads the filter chain graph 114 to the forwarding element 108. The forwarding element 108 applies the filter rules embodied in the filter chains 114 to all packets received and route the packets pursuant to the identifiers in the packet headers. According to Liu, the packet classification chains need not be "graph" or table form. Contrary to the contentions made in the Office Action, Liu fails to teach or suggest that a home agent may be configured to provide a signaling and tunneling functionality and to notify a proxy home agent of the mobile node as recited in independent claim 1. Accordingly, it is respectfully submitted that Liu does not disclose or suggest all of the elements of independent claim 1.

In addition, Liu does not cure the deficiencies of Adrangi. Similarly to Adrangi, Liu fails to disclose or suggest, at least, "the mobile node having only one security association and only one mobility binding with a home agent for the mobile internet home agent functionality," as recited in independent claim 1. Thus, the combination of Adrangi and Liu fail to teach or suggest all the recitations of independent claim 1 and related dependent claims.

It is respectfully submitted that independent claims 15, 19, and 20 include similar claim features as those recited in independent claim 1, and because the Office Action refers to similar portion of the cited references to reject independent claims 15, 19, and 20, the arguments presented above supporting the patentability of independent claim 1 are incorporated herein to support the patentability of independent claims 15, 19, and 20. It is respectfully requested that independent claims 1, 15, 19, and 20 and related dependent claims be allowed.

In response to the arguments section, on pages 16-17, the Office Action took the position that the combination of Adrangi and Liu disclose "wherein the HA is configured to provide a signaling and tunneling functionality and to notify the PHA of the mobile node." The Office Action cited Liu for allegedly disclosing "notifying the proxy home agent of the mobile node." However, Applicants respectfully disagree with the Office Action's position.

The cited portion of Liu does not disclose or suggest notifying the proxy home agent of the mobile node. Liu merely discloses that the remote endpoint 118 shown in FIG. 1A is connected to the local IPsec endpoints 102 through the forwarding element 108 in a data network device, which in this embodiment is an ON router 112. The forwarding element can be a combination of hardware and software configured to forward data. See column 2, lines 10-15, of Liu. There is no teaching or suggest in Liu of **notifying** the **proxy home agent of the mobile node**, as recited in the presently pending claims. (Emphasis Added). In Liu, A local IPsec endpoint 120 does not send a registration request, as asserted in the Office Action. Instead, the local IPsec endpoint 120 of Liu merely accesses public domain. See column 2, lines 10-11, of Liu. Thus, Liu fails to cure the deficiencies of Adrangi.

Similarly, as acknowledged in the Office Action, Adrangi fails to disclose notifying step. As such, the combination of Adrangi and Liu fails to disclose or suggest "wherein the HA is configured to provide a signaling and tunneling functionality and to notify the PHA of the mobile node," as recited in the presently pending claims. It is respectfully requested that the rejection of independent claims 1, 15, 19, and 20 and related dependent claims.

For the reasons explained above, it is respectfully submitted that each of claims 1-20 recites subject matter that is neither disclosed nor suggested in the prior art. It is, therefore, respectfully requested that all of claims 1-20 be allowed, and that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Sejoon Ahn
Registration No. 58,959

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

SA:dc